D

Notice of Allowability	**Application No.** 09/905,533	**Applicant(s)** JORDAN, MYLES	
	Examiner Michael Pyzocha	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed 10/31/2007*.

2. ☒ The allowed claim(s) is/are *1-3,5,7-13,15,17 and 18*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) □ All b) □ Some* c) □ None of the:
   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) □ hereto or 2) □ to Paper No./Mail Date _____.
   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 9/7/07
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Keiko Ichiye on 12/11/2007.

The application has been amended as follows:

11. (Currently Amended) An apparatus for detecting decryption of encrypted viral code in a subject file, comprising:

a processor; and

a storage device storing:

a code emulator, wherein the code emulator emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code; and

a memory monitor, wherein the memory monitor monitors the memory access information output by the code emulator, maintains a list of memory regions that have been read and then modified during the emulation, flags a memory area that is read during the emulation of a first instruction in the computer executable code, detects a modification to the flagged memory area during emulation of a second instruction in the computer executable code, updates the list of memory regions to include the modified flagged memory by:

determining whether the modified flagged memory area overlaps a listed memory region of the listed memory regions; and if the modified flagged memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified flagged memory area; and

if the modified flagged memory area does not overlap the listed memory region, adding the modified flagged memory area as a new memory region to the list of memory regions;

the memory monitor further determines that one of the listed memory regions is larger than a predetermined size, and triggers a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.

12. (Currently Amended) An apparatus for detecting decryption of encrypted viral code in a subject file, comprising:

a processor; and

a storage device storing:

a code emulator, wherein the code emulator emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code; and a memory monitor, wherein the memory monitor monitors the memory access information output by the code emulator, maintains a list of memory regions that have been read and modified during emulation, determines whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code, updates the list of memory regions to include the modified memory by:

determining whether the modified memory area overlaps a listed memory region of the listed memory regions; and

if the modified memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified memory area; and

if the modified memory area does not overlap the listed memory region, adding the modified memory area as a new memory region to the list of memory regions;

the memory monitor further determines that one of the listed memory regions is larger than a predetermined size, and triggers a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.

17. (Currently Amended) A storage medium which embodies instructions executable by a computer for detecting decryption of encrypted viral code in a subject file, comprising:

a first segment, including emulator code, wherein the emulator code emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code; and

a second segment including memory monitor code, wherein the memory monitor code monitors the memory access information output by the code emulator, maintains a list of memory regions that have been read and then modified during the emulation, flags a memory area that is read during the emulation of a first instruction in the computer executable code, detects a modification to the flagged memory area during emulation of a second instruction in the computer executable code, updates the list of memory regions to include the modified flagged memory by:

determining whether the modified memory area overlaps a listed memory region of the listed memory regions; and if the modified memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified memory area; and

if the modified memory area does not overlap the listed memory region, adding the modified memory area as a new memory region to the list of memory regions;

the memory monitor code further determines that one of the listed memory regions is larger than a predetermined size, and triggers a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the ~viral detection alarm indicating detection of viral code.

18. (Currently Amended) A <u>storage</u> medium which embodies instructions executable by a computer for detecting encrypted viral code in a subject file, comprising:

a first segment including emulator code, wherein the emulator code emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code; and

a second segment including memory monitor code, wherein the memory monitor code monitors the memory access information output by the code emulator, maintains a list of memory regions that have been read and modified during emulation, determines whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code, updates the list of memory regions to include the modified memory by:

determining whether the modified memory area overlaps a listed memory region of the listed memory regions; and

if the modified memory area overlaps the listed memory region, updating a dimension of the listed memory region to encompass the modified memory area; and

if the modified memory area does not overlap the listed memory region, adding the modified memory area as a new memory region to the list of memory regions;

the memory monitor code further determines that one of the listed memory regions is larger than a predetermined size, and triggers a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.

2. The following is an examiner's statement of reasons for allowance: The prior art teaches flagging memory areas (see Nachenberg US 5826013 and 5765030), but fails to teach updating a dimension of the listed memory region to encompass the modified memory area as taught in each of the independent claims.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER